Amendment To The Claims:

Claims 1-29 Canceled.

30. (New) A content processing unit for protecting interchip content pathways transporting content, the content processing unit comprising:

a first chip package which receives content, wherein the first chip package comprises:

a first body,

an encryption engine, and

a first key storage register capable of storing an interchip key,

wherein:

the interchip key is used by the encryption engine to produce ciphertext content from the received content,

the first key storage register is non-readable from outside the first body, and

the first key storage register cannot be overwritten after a programmability period, the programmability period being a period in which the interchip key is loaded in the first key storage,

a second chip package, wherein the second chip package comprises:

a second body,

a decryption engine, and

a second key storage register capable of storing the interchip key,

wherein:

the interchip key is used by the decryption engine to produce plaintext content from the ciphertext content received from the first chip package, and

the second key storage register is non-readable from outside the second body, the second key storage register being writeable while being non-readable; and

an interchip content pathway connecting the first chip package and the second chip package within said content processing unit, the interchip content pathway carrying the ciphertext content from the first chip package to the second chip package; and

an output configured to provide the plaintext content to a user device capable of providing content to a user.

31. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 30, further the first chip package includes a fusable link, wherein the first key storage register cannot be overwritten after the fusable link is activated.

32. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 30, wherein the programmability period ends after writing to the first key storage register.

33. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 30, wherein at least one of the first and second chip packages comprises a plurality of semiconductor substrates.

34. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 30, wherein:

the first chip package further stores a key encryption key,

the interchip key is encrypted with the key encryption key, and

the second chip package obtains the interchip key by decrypting the interchip key using the key encryption key.

35. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 34, further comprising a plurality of content processing chip packages, each content processing chip package of the plurality of content processing chip packages having a unique key as the key encryption key, the unique key of each content processing chip package being distinct from the unique key of each other content processing chip package.

36. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 35, wherein each of the plurality of content processing chip packages receives a ciphertext message and obtains a unique interchip key by using the unique key to decrypt the message, the unique interchip key of each content processing chip package being distinct from the unique interchip key of each other content processing chip package.

37. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 30, wherein the second key storage register is overwritable.

38. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 30, wherein:

the second chip package further comprises a second encryption engine, and

the second encryption engine uses the interchip key or another key that is a function of the interchip key.

39. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 36, further comprising a third chip package comprising a second interchip key that can decrypt second ciphertext content produced with the second encryption engine at the second chip package.

40. (New) The content processing unit for protecting interchip content pathways transporting content as recited in claim 37, wherein the third chip package is connected to the second chip package by a second interchip content pathway, the second interchip content pathway carrying the second ciphertext content from the first chip package to the second chip package.

41. (New) A method for protecting interchip content pathways transporting content within a content processing unit, the method comprising steps of:

loading an interchip key into a first key storage register in a first chip package, wherein the interchip key in the first key storage register is non-readable from outside the first chip package;

activating a feature of the first chip package that prevents overwriting the interchip key in the first key storage register from outside the first chip package, after a period in which the first key is loaded in the first key storage;

encrypting digital content with the interchip key to produce ciphertext content;

coupling the ciphertext content from the first chip package to a content pathway;

loading the interchip key into a second key storage register in a second chip package, wherein the interchip key in the second key storage register is non-readable from outside the second chip package, the second key storage register being writeable while being non-readable;

coupling the ciphertext content from the content pathway to a second chip package; and

decrypting the ciphertext content with the interchip key to reformulate the digital content.

42. (New) The method of claim 41, further comprising steps of:

loading a key encryption key into the first chip package; and

decrypting the interchip key with the key encryption key, whereby the interchip key is protected with the key encryption key outside the first chip package.

43. (New) The method of claim 41, further comprising a step of overwriting the interchip key in the second key storage register from outside the second chip package.

44. (New) The method of claim 41, further comprising steps of:

encrypting the digital content in the second chip package to produce second ciphertext content using a second interchip key,

coupling the second ciphertext content to a second content pathway.

45. (New) The method of claim 41, further comprising:

providing a unique interchip key to each of a plurality of content processing chip packages, the unique interchip key of each content processing chip package being distinct from

the unique key of each other content processing chip package and protecting a respective content pathway to each content chip processing package.

46. (New) The method of claim 45, wherein the step of providing a unique interchip key includes providing a message to each of the plurality of content processing chip packages, and each content processing chip package decrypts the message to obtain a unique interchip key.

47. (New) A computer readable medium containing instructions for a computer to perform a method for protecting interchip content pathways transporting content within a content processing unit, the method comprising steps of:

loading an interchip key into a first key storage register in a first chip package, wherein the interchip key in the first key storage register is non-readable from outside the first chip package;

activating a feature of the first chip package that prevents overwriting the interchip key in the first key storage register from outside the first chip package, after a period in which the first key is loaded in the first key storage;

encrypting digital content with the interchip key to produce ciphertext content;

coupling the ciphertext content from the first chip package to a content pathway;

loading the interchip key into a second key storage register in a second chip package, wherein the interchip key in the second key storage register is non-readable from outside the second chip package, the second key storage register being writeable while being non-readable;

coupling the ciphertext content from the content pathway to a second chip package; and

decrypting the ciphertext content with the interchip key to reformulate the digital content.

48. (New) The computer readable medium of claim 47, further comprising instructions to perform steps of:

loading a key encryption key into the first chip package; and

decrypting the interchip key with the key encryption key, whereby the interchip key is protected with the key encryption key outside the first chip package.

49. (New) The computer readable medium of claim 47, further comprising instructions to perform a step of overwriting the interchip key in the second key storage register from outside the second chip package.

50. (New) The computer readable medium of claim 47, further comprising steps of:

encrypting the digital content in the second chip package to produce second ciphertext content using a second interchip key,

coupling the second ciphertext content to a second content pathway.

51. (New) The computer readable medium of claim 47, further comprising instructions to perform a step of:

providing a unique interchip key to each of a plurality of content processing chip packages, the unique interchip key of each content processing chip package being distinct from the unique key of each other content processing chip package and protecting a respective content pathway to each content chip processing package.

52. (New) The computer readable medium of claim 51, wherein the step of providing a unique interchip key includes providing a message to each of the plurality of content processing chip packages, and each content processing chip package decrypts the message to obtain a unique interchip key a unique key encrypting key.